PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-180010

(43)Date of publication of application : 24.06.2004

---

(51)Int.Cl. H04L 12/28
H04L 9/32
H04Q 7/38

---

(21)Application number : 2002-344286 (71)Applicant : CANON INC

(22)Date of filing : 27.11.2002 (72)Inventor : HIROSE TAKATOSHI

---

(54) TERMINAL UNIT FOR RADIO COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a terminal unit for radio communication that easily joins a network, even if identification information of a radio access point, with which the unit desires to communicate with, is changed.

SOLUTION: When a radio station terminal STA1 sends an authentication requesting message by using SS-ID "11111", a radio access point AP1 holding "11111" conducts authentication processing between the terminal STA1 and the point. However, since the WEP keys, respectively set to the terminal and the point, are different from each other, an authentication-denying message is returned. Then, the terminal STA1 receives beacon signals sent from a plurality of radio access points AP, keeps SS-IDs and receiving electric field intensities contained in the signals in a data base 801, and selects the SS-ID having the strongest receiving electric field strength among the SS-IDs except erroneously authenticated SS-IDs as a new SS-ID. In

addition, the terminal makes an authentication request, using the newly set SS-ID.

LEGAL STATUS [Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1]
It is the radio terminal unit which performs a secrecy communication link with the wireless access point of said request using the same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points,
An identification information setting means to set up the identification information for authentication processing,
The authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means among said two or more wireless access

points,

It has an information signal receiving means to receive the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points,

It is the radio terminal unit characterized by changing a setup into the identification information which received with said information signal receiving means, and carrying out authentication processing when authentication processing goes wrong.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The field of the technique in which invention belongs]

This invention relates to the technique at the time of performing a wireless access point and data communication.

[0002]

[Description of the Prior Art]

Conventionally, the wireless access point and the radio terminal unit which performs a secrecy communication link are known using the same cryptographic keys, such as a WEP (Wired Equivalent Privacy) key.

[0003]

For example, by the following patent reference 1, after a wireless access point performs "Shared Key authentication" from a wireless station terminal, the technique of raising the security level of authentication processing is shown by obtaining final authorization of authentication to a network administrator.

[0004]

That is, in a wireless LAN system, as shown in drawing 2 , three wireless access points AP1, AP2, and AP3 are working, respectively, and the case where the wireless station terminal STA 1 which is a radio terminal unit is going to communicate after this is assumed. The wireless access points AP1, AP2, and AP3 hold mutually different SS-ID (Sevice Set Identifier) as system identification information. Each SS-ID presupposes that it is "33333" in "11111" and the wireless access point AP 2 by the wireless access point AP 1 in "22222" and the wireless access point AP 3. Each wireless area (range which a radio signal reaches) of the wireless access points AP1-AP3 is shown by 206, 207, and 208. The wireless station terminal STA 1 presupposes that it exists within the limits of current and all the wireless area 206, 207, and 208.

[0005]

Now, supposing SS-ID set as the wireless station terminal STA 1 is "11111", the wireless station terminal STA 1 can communicate with the wireless access point AP 1 where SS-ID is common, and supposing it is "22222", supposing it is "33333", it can communicate with the wireless access point AP 3 to the wireless access point AP 2 and a pan. Moreover, a communications partner will be found when other SS-ID is used. It turns out by using an authentication sequence that it is such.

[0006]

Two kinds of authentication sequences defined by wireless LAN specification IEEE802.11 exist, and are called "Open System authentication" and "Shared Key authentication", respectively. Each big difference is whether to use the secrecy communication link which used WEP (WiredEquivalent Privacy) at the time of authentication. Even if "Open System authentication" does not use WEP, it is possible, and "Shared Key authentication" uses WEP. [of an authentication sequence]

[0007]

Here, the WEP algorithm of IEEE802.11 is explained using drawing 6 and drawing 7 .

[0008]

Drawing 6 is drawing showing the configuration of the encryption equipment in a WEP algorithm. Drawing 7 is drawing showing the configuration of the decode equipment in a WEP algorithm. These encryption equipment and decode equipment are formed in the wireless station terminal STA and the wireless access point AP.

[0009]

As shown in drawing 6 , encryption equipment combines two inputted bit strings, and is equipped with the couplers 601 and 604 made into one bit string. The pseudo-random-number generator 602 uses the result of a coupler 601 as a seed, and generates a longer bit sequence (key sequence) using a pseudo-random-number generating algorithm. CRC equipment 603 generates the bit string (ICV) which confirms whether an error is in a bit string using a CRC (Cyclic Redundancy Check) algorithm. XOR equipment 605 searches for the exclusive OR of two inputted bit sequences. As a pseudo-random-number generating algorithm, RC4 pseudo-random-number generating algorithm of a RSA security company is used.

[0010]

The initialization sequence which is a bit string of arbitration, a cryptographic key, and the data enciphered are inputted into the encryption equipment shown in drawing 6 . An initialization sequence and a cryptographic key are inputted into a coupler 601, and the kind which is the bit sequence which combined the initialization sequence and the cryptographic key is outputted. This kind is inputted into the pseudo-random-number generator 602, and the key sequence which is a bit sequence of the die length which applied the die length of data and the die length of ICV is generated. Moreover, data are inputted into CRC equipment 603 and ICV is generated. Data and generated ICV

are inputted and combined with a coupler 604. The key sequence outputted to ICV outputted from a coupler 604 and association of data, and a list from the pseudo-random-number generator 602 is inputted into XOR equipment 605, and the exclusive OR for every bit is taken. The result of having taken the exclusive OR with XOR equipment 605 serves as encryption data. And an initialization sequence and encryption data are made into a lot, and are outputted.

[0011]

Moreover, as shown in drawing 7 , decode equipment combines two inputted bit strings, and is equipped with the coupler 701 made into one bit string. The pseudo-random-number generator 702 uses the result of a coupler 701 as a seed, and generates a longer bit sequence (key sequence) using a pseudo-random-number generating algorithm. XOR equipment 703 searches for the exclusive OR of two inputted bit sequences. An eliminator 704 is a predetermined approach and divides the inputted bit string into two bit strings, data and ICV. CRC equipment 705 generates ICV using a CRC algorithm. When the judgment machine 706 compares ICV generated by the eliminator 704 with ICV generated with CRC equipment 705, data judge whether it is the right. As a pseudo-random-number generating algorithm, RC4 pseudo-random-number generating algorithm of a RSA security company etc. is used.

[0012]

The group of encryption data and an initialization sequence and a cryptographic key are inputted into the decode equipment shown in drawing 7 . An initialization sequence and a cryptographic key are inputted into a coupler 701, and the kind which is the bit sequence which combined the initialization sequence and the cryptographic key is outputted. This kind is inputted into the pseudo-random-number generator 702, and the key sequence which is a bit sequence of the die length which applied the die length of data and the die length of ICV is generated. This key sequence and the above-mentioned encryption data are inputted into XOR equipment 703, and the exclusive OR for every bit is calculated. The count result of XOR equipment 703 is inputted into an eliminator 704, is divided by the predetermined approach, and data and ICV are generated. While this data is outputted, ICV is calculated by being inputted into CRC equipment 705. ICV calculated with CRC equipment 705 and ICV generated by the eliminator 704 are inputted into judgment equipment 706. With judgment equipment 706, if these two ICV(s) are equal and it is not equal in the flag which shows normal decode as a judgment flag, the flag which shows decode failure is outputted.

[0013]

The association sequence performed following the sequence and authentication sequence of "Shared Key authentication" which used this WEP for authentication processing is explained using drawing 3 .

[0014]

First, the wireless station terminal STA transmits the authentication demand message 301 to the wireless access point AP. Into the message 301, using "Shared Key authentication" as an authentication algorithm describes.

[0015]

The wireless access point AP which received it transmits the authentication response message 302 to the wireless station terminal STA. Into that message 302, IV (Initialization Vector) which can be decided to be arbitration at every authentication procedure of this, and the value of a WEP key are made into a parameter, and it is WEP. Challenge performs math processing according to the algorithm of PRNG (Pseudorandom Number Generator), and it is decided that will be the meaning of 128 octets What computed the value of Text is contained.

[0016]

Challenge The wireless station terminal STA which received the message 302 containing Text is Challenge. To Text data, it enciphers according to WEP encryption algorithm, and transmits to the wireless access point AP by making the encryption data into the authentication demand message 303.

[0017]

The wireless access point AP which received the message 303 decrypts encryption data based on notified IV and the WEP key data known beforehand. And if ICV it was notified that was the output ICV at the time of decrypting is the same, it will consider as authentication authorization and will transmit to the wireless station terminal STA as an authentication response message 304.

[0018]

Consequently, if it is authentication authorization, the wireless station terminal STA can go into the procedure of the next association, and when it is authentication refusal, association procedure cannot be performed by authentication failure.

[0019]

Next, the association sequence performed following an authentication sequence is explained.

[0020]

As shown in drawing 3 , the wireless station terminal STA transmits the association demand message 305 to the wireless access point AP.

[0021]

It is determined whether the wireless access point AP which received SS-ID in the association demand message 305 permits the association according to the association authorization Ruhr which identified the wireless station terminal STA by above-mentioned SS-ID, and was decided beforehand. And when granting a permission, the association response message 306 of association authorization is transmitted to the wireless station terminal STA.

[0022]

Thus, by being processed, the wireless access point AP and the radio link between the wireless station terminals STA can be stretched (data link establishment 307), and a communication link becomes possible. That is, according to this authentication and association approach, the structure which the wireless access point AP permits authentication and an association to the specific wireless station terminal STA because the wireless access point AP and the wireless station terminal STA share each other's WEP keys with SS-ID beforehand is realized.

[0023]

[Patent reference 1]

JP,2001-345819,A

[0024]

[Problem(s) to be Solved by the Invention]

However, a setup of SS-ID in the wireless access point AP may be changed for the reasons of SS-ID having lapped with other SS-ID in fact on the occasion of wireless access point AP installation by the conventional authentication and association technique shown in the above-mentioned patent reference 1 grade, although radio could be performed when the wireless access point AP and the wireless station terminal STA shared each other's respectively same SS-ID and WEP keys. And even if it was such a case, in the wireless station terminal STA side, it became impossible it to usually come out not to know the modification and it to perform radio for a certain reason, and there was a problem that the participation to a network was not easy.

[0025]

It is made in order that this invention may solve the problem of the above-mentioned conventional technique, and the purpose is in enabling it to participate in a network easily, even if the identification information of a wireless access point which wishes to communicate is changed.

[0026]

[Means for Solving the Problem]

In order to attain the above-mentioned purpose the radio terminal unit of claim 1 of this invention The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. An identification information setting means to be the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and to set up the identification information for authentication processing, The authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means among said two or more wireless access points, It has an information signal receiving means to receive the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points. When authentication processing goes wrong,

it is characterized by changing a setup into the identification information which received with said information signal receiving means, and carrying out authentication processing.

[0027]

[Embodiment of the Invention]

Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.

[0028]

Drawing 1 is the block diagram showing the configuration of the radio terminal unit concerning the gestalt of 1 operation of this invention. the wireless station terminal STA which is a radio terminal unit -- the wireless transceiver section 102 (information signal receiving means), the storage section 103 (identification information storage means), the network interface processing section 104, and a time check -- it has the section 105, a control section 106 (an identification information setting means, authentication demand means), and a display 107 (identification information display means).

[0029]

In addition, the wireless station terminal STA and the wireless access point AP have the encryption equipment and decode equipment which are shown in drawing 6 and drawing 7 . Moreover, each wireless station terminal STAs and each wireless access point AP are constituted similarly.

[0030]

Drawing 2 is a wireless LAN structure-of-a-system Fig. built in the wireless station terminal STA and the wireless access point AP. The gestalt of this operation describes the example which uses wireless LAN as a wireless conference system.

[0031]

Although illustration is not carried out, it shall connect with a personal computer (PC), and shall connect also with the projector further, and the wireless station STA 2 shall project PC screen on a screen etc.

[0032]

Moreover, although the participant at a wireless meeting has the wireless station terminal STA connected to PC, respectively, in subsequent explanation, a participant presupposes that it is only the user 1 name of the wireless station terminal STA 1. Moreover, the wireless access point of a wireless conference system presupposes that it is the wireless access point AP 3, and the wireless access point AP 1 and the wireless access point AP 2 are working as other wireless access points.

[0033]

With the gestalt of this operation, the user of the wireless station terminal STA 1 explains the authentication and the association procedure between the wireless access point AP3-wireless station terminals STA 1 in the case of carrying out a

presentation using the projector connected to the wireless station terminal STA 2 via the wireless access point AP 3. In addition, suppose that "11111" is used at the beginning as SS-ID set as the wireless access point AP 3 at this wireless meeting.

[0034]

Moreover, with the gestalt of this operation, it shall attest according to "Shared Key authentication" using WEP (Wired Equivalent Privacy) which is one of the authentication sequences defined by wireless LAN specification IEEE802.11. The encryption equipment and decode equipment which were shown in drawing 6 and drawing 7 shall be formed in each wireless station terminal STA and each wireless access point AP. In addition, it is as having mentioned above by drawing 6 and drawing 7 about the WEP algorithm.

[0035]

First, in advance of a meeting, the wireless access point AP 3 and the wireless station terminal STA 1 are set up about a need item, respectively. Need setting items are SS-ID, a WEP key (cryptographic key), etc. About a WEP key, the same thing is set up at the wireless access point AP 3 and the wireless station terminal STA 1. To a setup, various approaches are possible and the wireless access point AP 3 and the wireless station terminal STA 1 can also carry out separately. Moreover, it is possible to set up, even if it is not a meeting location.

[0036]

Here, "11111" was set to the wireless access point AP 3 as SS-ID until it went to the meeting location, but since the thing SS-ID"11111" was used by the wireless access point AP 1 near the meeting location, the case where SS-ID of the wireless access point AP 3 is changed into "33333" hurriedly is assumed. Consequently, SS-ID of each wireless access point AP became "11111" in the wireless access point AP 1, and became "33333" in "22222" and the wireless access point AP 3 in the wireless access point AP 2. Naturally modification of SS-ID in the wireless access point AP 3 is not told to the wireless station terminal STA 1.

[0037]

In this situation, processing in case the wireless station terminal STA 1 participates in a wireless meeting is explained using drawing 4 and drawing 5 .

[0038]

Drawing 4 shows the sequence of authentication and association processing, and drawing 5 shows the flow chart of authentication and association processing. Processing of drawing 5 is performed by the control section 106. Henceforth, it explains with reference to both.

[0039]

The wireless access point AP 3 is installed in a meeting location, first, the wireless station terminal STA 1 comes to a meeting location by the condition that the wireless access point AP 3 is working, and the power source is turned on in it (401 step S501).

And those setup is performed when SS-ID, a WEP key, etc. are not beforehand set as the wireless station terminal STA 1 (step S502).

[0040]

Next, at the wireless station terminal STA 1, in order to notify the user of the wireless station terminal STA 1 of it being in the condition prepared for stretching a radio link with the wireless access point AP, an indication "under communication link setup" is given to a display 107 (step S503). Moreover, all elimination of the contents of the database 801 (refer to drawing 8) which is memorized by the storage section 103 and which is mentioned later is performed. Here, SS-ID of the wireless station terminal STA 1 is set as "11111" of the original schedule.

[0041]

Drawing 8 is drawing showing an example of a database 801. While the received field strength is matched and memorized by SS-ID of the wireless access point AP obtained by reception of the beacon signal (information signal) mentioned later etc., when authentication processing fails in a database 801 using the SS-ID, the information which shows authentication processing failure is matched and it memorizes.

[0042]

Return, next the wireless station terminal STA 1 give an authentication demand to drawing 4 and drawing 5 , in order to stretch a radio link (402). These processings are made in the procedure mentioned above by drawing 3 . Namely, Shared Key authentication is chosen and an authentication demand message is sent out by SS-ID"11111" (402). And it distinguishes whether authentication and an association were permitted (step S504).

[0043]-

On the other hand, the wireless access point AP 1 which holds SS-ID"11111" receives the sent-out authentication demand message (402), and performs authentication processing between the wireless station terminals STA 1.

[0044]

However, since the WEP keys set as each in the wireless station terminal STA 1 and the wireless access point AP 1 differ, the wireless access point AP 1 transmits an authentication refusal message to the wireless station terminal STA 1 (403).

[0045]

Therefore, it is set to "NO" in this case as a result of distinction of said step S504. and SS-ID of the wireless access point AP 1 of authentication failure in the database 801 in the storage section 103 of the wireless station terminal STA 1 -- "11111" is kept with the check of authentication processing failure. and a time check -- a time check is started by the section 105 (404).

[0046]

Next, the wireless station terminal STA 1 is performed until a timer ends scanning

(Scanning) actuation (407) which receives the beacon signal sent out from two or more wireless access points AP (409). Here, the beacon signal sent from all the wireless access points AP of the wireless access points AP1-AP3 is received.

[0047]

In this scanning actuation (407), SS-ID and received field strength of the wireless access point AP included in a receiving beacon signal are kept by the database 801 in the storage section 103 of the wireless station terminal STA 1 (405, 406, 408). When data are in a database 801, the data and OR are taken.

[0048]

At step S505, when it distinguishes whether the beacon signal was received and a beacon signal cannot be received, the user of the wireless station terminal STA 1 is notified of making a display 107 indicate by the "outside of the circle" (step S512), and the wireless access point AP not existing in it.

[0049]

On the other hand, when a beacon signal is receivable, SS-ID is rearranged in order of the received field strength (step S508), and SS-ID with the largest received field strength is chosen as SS-ID set as the wireless station terminal STA 1, and is set up (step S507). However, when SS-ID to which the check is attached to the column of authentication processing failure of a database 801 exists, authentication processing which used it is not performed. Authentication processing which used SS-ID"11111" is not performed in the example of drawing 8 . That is, SS-ID with the largest received field strength is chosen among the things except SS-ID concerning authentication processing failure. Consequently, SS-ID"22222" is chosen and set up in the example of drawing 8 .

[0050]

Next, the wireless station terminal STA 1 performs an authentication demand in newly set-up SS-ID, in order to stretch a radio link (410). Namely, Shared Key authentication is chosen and an authentication demand message is sent out by SS-ID"22222" (410). And it distinguishes whether authentication and an association were permitted (step S508).

[0051]

On the other hand, the wireless access point AP 2 which holds SS-ID"22222" receives the sent-out authentication demand message (410), and performs authentication processing between the wireless station terminals STA 1.

[0052]

However, since the WEP keys set as each in the wireless station terminal STA 1 and the wireless access point AP 2 differ, the wireless access point AP 2 transmits an authentication refusal message to the wireless station terminal STA 1 like the case of the wireless access point AP 1 (411).

[0053]

Therefore, it is set to "NO" in this case as a result of distinction of said step S508. and SS-ID of the wireless access point AP 2 of authentication failure in the database 801 in the storage section 103 of the wireless station terminal STA 1 -- "22222" is kept with the check of authentication processing failure. When data are in a database 801, the data and OR are taken.

[0054]

Next, with reference to a database 801, it distinguishes whether the next candidate SS-ID exists (step S509). That is, it checks whether there is other SS-ID which the check of authentication processing failure does not attach to a database 801.

[0055]

When the candidate of following SS-ID does not exist as a result of the distinction, wireless station terminal STA1 user is notified of (step S512) and the wireless access point AP which can communicate not existing by indicating to a display 107 by the "outside of the circle."

[0056]

next -- step S513 -- a time check -- the section 105 -- an outside-of-the-circle timer -- a time check is started and it distinguishes whether the outside-of-the-circle timer passed the deadline of (step S514).

[0057]

When the distinction is repeated and an outside-of-the-circle timer passes the deadline of until an outside-of-the-circle timer passes the deadline of, it returns to said step S503, and it is giving an indication "under communication link setup" to a display 107, and shifts to authentication processing for the second time. Since reconfirmation certificate processing is not immediately performed but it waits for the fixed passage of time by this even when the wireless station terminal STA 1 becomes outside the circle with an outside-of-the-circle timer, sending out of a dc-battery or an electric wave can be suppressed.

[0058]

When the candidate of following SS-ID exists as a result of distinction of said step S509, it returns to said step S507. In this case, SS-ID"33333" is chosen and set up. And the wireless station terminal STA 1 shifts to authentication and association processing similarly (412). These processings are made in the procedure mentioned above by drawing 3 . First, an authentication demand is performed in order to stretch a radio link. Namely, Shared Key authentication is chosen, an authentication demand message is sent out by SS-ID"33333", and it distinguishes whether authentication and an association were permitted (step S508).

[0059]

On the other hand, the wireless access point AP 3 which holds SS-ID"33333" receives the sent-out authentication demand message, and performs authentication processing between the wireless station terminals STA 1.

[0060]
Here, since the WEP key set as each in the wireless station terminal STA 1 and the wireless access point AP 3 is the same, as for the wireless access point AP 3, an authentication allowed message is transmitted to the wireless station terminal STA 1. Furthermore, the wireless station terminal STA 1 and the wireless access point AP 3 perform association processing. Thereby, a wireless data link is established (413).
[0061]
Then, it is set to "YES" at said step S508, and "selected SS-ID" is displayed on a display 107 at the wireless station terminal STA 1 (step S510). Then, "under a communication link" is displayed on a display 107 (step S511), and this processing is ended.
[0062]
In addition, when distinguished from "YES" as a result of distinction of said step S504, said steps S510 and S511 are performed, and this processing is ended.
[0063]
By receiving SS-ID in the beacon signal with which the wireless station terminal STA is sent out from the wireless access point AP according to the gestalt of this operation, SS-ID set as the wireless access point AP is known, and it is Shared of IEEE802.11. Since by performing Key authentication shows the correction of a WEP key, even if SS-ID of the wireless access point AP which wants to communicate is changed, authentication and an association with the wireless access point AP are easily securable. Therefore, the need of not necessarily setting up SS-ID is lost, and it can participate now in a network easily.
[0064]
In addition, with the gestalt of this operation, although illustrated about the case in a wireless conference system, the same technique is applicable also about the radio when not being a wireless conference system. Moreover, it is effective also at the wireless station where neither a timer nor a display exists.
[0065]
Moreover, the approach of choosing as SS-ID which newly sets up SS-ID which received also besides choosing from SS-ID with the largest received field strength as newly set-up SS-ID at random can be considered.
[0066]
In addition, with the gestalt of this operation, although the wireless station terminal STA 1 illustrated the authentication and association processing between the wireless access points AP 3, between other wireless station terminals STA and the wireless access point AP is processed similarly.
[0067]
Moreover, the purpose of this invention supplies the storage which recorded the program code of the software which realizes the function of the gestalt of operation

to a system or equipment, and is attained also by reading and performing the program code with which the computers (or CPU, MPU, etc.) of the system or equipment were stored in the storage.

[0068]

In this case, the function of the gestalt of operation which the program code itself read from the storage mentioned above will be realized, and the storage which memorized that program code will constitute this invention.

[0069]

Moreover, as a storage for supplying a program code, a floppy (trademark) disk, a hard disk, a magneto-optic disk, CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM, DVD-RW, DVD+RW, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.

[0070]

Moreover, by performing the program code which the computer read, a part or all of processing that OS (operating system) which the function of the gestalt of the above-mentioned implementation is not only realized, but is working on a computer based on directions of the program code is actual is performed, and also when the function of the operation gestalt mentioned above by the processing is realized, it is contained.

[0071]

Furthermore, after the program code read from the storage is written in the memory with which the functional expansion unit connected to the functional add-in board inserted in the computer or the computer is equipped, a part or all of processing that CPU with which the functional add-in board and functional expansion unit are equipped is actual performs, and also when the function of the operation gestalt mentioned above by the processing is realized, it is contained based on directions of the program code.

[0072]

Although various examples and examples of this invention were shown and it was explained, if it is this contractor, the meaning and the range of this invention will not be limited to specific explanation of this specification and drawing, but attaining to various corrections altogether stated to the range which is this application application for patent, and modification will be understood.

[0073]

The examples of the embodiment of this invention are enumerated below.

[0074]

[Embodiment 1] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. An identification information setting means to be the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and

to set up the identification information for authentication processing. The authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means among said two or more wireless access points, It has an information signal receiving means to receive the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points. Said identification information setting means is a radio terminal unit characterized by setting up the identification information in the information signal received by said information signal receiving means as identification information for said authentication processing.

[0075]

[Embodiment 2] Said information signal receiving means is the radio terminal unit of the embodiment 1 publication characterized by receiving said information signal when authentication is not acquired from said wireless access point to the authentication demand by said authentication demand means.

[0076]

[Embodiment 3] Said identification information setting means is the embodiment 1 characterized by choosing the identification information used for a setup as identification information for said authentication processing based on the received field strength at the time of said information signal being received when an information signal is received from two or more wireless access points, or a radio terminal unit given in two.

[0077]

[Embodiment 4] It has an identification information storage means to memorize the identification information in the information signal received by said information signal receiving means. Said identification information setting means When authentication is not acquired from said wireless access point to the authentication demand by said authentication demand means A radio terminal unit given in either of the embodiments 1-3 characterized by resetting different identification information from the identification information set up as identification information for authentication processing among the identification information memorized by said identification information storage means before last time as new identification information for authentication processing.

[0078]

[Embodiment 5] Said identification information setting means about all the identification information memorized by said identification information storage means As a result of performing resetting as said new identification information for authentication processing and said authentication demand means' performing an authentication demand, when authentication is not acquired from any wireless access point Said information signal receiving means is the radio terminal unit of the

embodiment 4 publication characterized by redoing reception of said information signal again after fixed time amount progress.

[0079]

[Embodiment 6] It is a radio terminal unit given in either of the embodiments 1–5 characterized by having an identification information display means to display the identification information set up by said identification information setting means in that case when authentication is acquired from said wireless access point to the authentication demand by said authentication demand means.

[0080]

[Embodiment 7] The authentication by said wireless access point is Shared defined by wireless specification IEEE802.11. Key Radio terminal unit given in either of the embodiments 1–6 characterized by being made according to Authentication.

[0081]

[Embodiment 8] Said secrecy communication link is a radio terminal unit given in either of the embodiments 1–7 characterized by being made by WEP (Wired Equivalent Privacy) defined by wireless specification IEEE802.11.

[0082]

[Embodiment 9] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points and said two or more wireless access points is used. It is the radio communications system to which the wireless access point of said request and the radio terminal unit which performs a secrecy communication link were connected. Said two or more wireless access points The authentication means which attests using said cryptographic key according to the authentication demand from said radio terminal unit, It has an information signal dispatch means to send the information signal containing the identification information set as each wireless access point. Said radio terminal unit An identification information setting means to set up the identification information for authentication processing, and the authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means among said two or more wireless access points, It has an information signal receiving means to receive said information signal sent from said two or more wireless access points. Said identification information setting means The radio communications system characterized by setting up the identification information in the information signal received by said information signal receiving means as identification information for said authentication processing.

[0083]

[Embodiment 10] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is a correspondence procedure in the

wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and sets up the identification information for authentication processing, The authentication demand step which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, It has the information signal receiving step which receives the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points. Said identification information setting step is a correspondence procedure characterized by setting up the identification information in the information signal received by said information signal receiving step as identification information for said authentication processing.

[0084]

[Embodiment 11] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is a communications program in the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and sets up the identification information for authentication processing, The authentication demand step which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, It is the program which makes a computer perform the information signal receiving step which receives the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points. Said identification information setting step is a communications program characterized by setting up the identification information in the information signal received by said information signal receiving step as identification information for said authentication processing.

[0085]

[Embodiment 12] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is the storage which memorized the communications program in the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and in which computer reading is possible, and sets up the identification information for authentication processing, The authentication demand step which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, The program which makes a computer perform the information signal receiving step which receives the information signal containing the identification

information set as each wireless access point sent from said two or more wireless access points is memorized. Said identification information setting step is a storage characterized by setting up the identification information in the information signal received by said information signal receiving step as identification information for said authentication processing.

[0086]

[Operation gestalt 13] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. An identification information setting means to be the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and to set up the identification information for authentication processing, The authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means among said two or more wireless access points, It has an information signal receiving means to receive the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points. It is the radio terminal unit characterized by changing a setup into the identification information which received with said information signal receiving means, and carrying out authentication processing when authentication processing goes wrong.

[0087]

[Operation gestalt 14] An identification information setting means to perform a secrecy communication link with said wireless access point using the same cryptographic key as the cryptographic key which a wireless access point holds and to be a radio terminal unit and to set up the identification information for authentication processing, The authentication demand means which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting means, When it has an information signal receiving means to receive the information signal containing the identification information set as other wireless access points and authentication processing with said wireless access point goes wrong The radio terminal unit characterized by changing a setup into the identification information which received with said information signal receiving means, and carrying out authentication processing.

[0088]

[Embodiment 15] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is a correspondence procedure in the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and sets up the identification information for authentication processing, The authentication demand step which carries out an

authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, The information signal receiving step which receives the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points, It is a correspondence procedure in the radio terminal unit characterized by having the authentication processing step which changes a setup into the identification information which received with said information signal receiving means, and carries out authentication processing when authentication processing goes wrong.

[0089]

[Embodiment 16] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is a communications program in the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and sets up the identification information for authentication processing, The authentication demand step which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, The information signal receiving step which receives the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points, It is the communications program characterized by making a computer perform the authentication processing step which changes a setup into the identification information which received with said information signal receiving means, and carries out authentication processing when authentication processing goes wrong.

[0090]

[Embodiment 17] The same cryptographic key as the cryptographic key which a desired wireless access point holds among two or more wireless access points is used. The identification information setting step which is the storage which memorized the communications program in the wireless access point of said request, and the radio terminal unit which performs a secrecy communication link, and in which computer reading is possible, and sets up the identification information for authentication processing, The authentication demand step which carries out an authentication demand to the wireless access point corresponding to the identification information set up by said identification information setting step among said two or more wireless access points, The information signal receiving step which receives the information signal containing the identification information set as each wireless access point sent from said two or more wireless access points, It is the storage characterized by memorizing the program which makes a computer perform the authentication processing step which changes a setup into the identification information which

received with said information signal receiving means, and carries out authentication processing when authentication processing goes wrong.

[0091]

[Effect of the Invention]

As explained above, even if the identification information of a wireless access point which wishes to communicate is changed according to this invention, it can participate in a network easily by acquiring authentication by the identification information acquired from the information signal.

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of the radio terminal unit concerning the gestalt of 1 operation of this invention.

[Drawing 2] It is the wireless LAN structure-of-a-system Fig. built in the wireless station terminal STA and the wireless access point AP.

[Drawing 3] It is drawing showing the association sequence performed following the sequence and authentication sequence of "Shared Key authentication" which used WEP for authentication processing.

[Drawing 4] It is drawing showing the sequence of authentication and association processing.

[Drawing 5] It is drawing showing the flow chart of authentication and association processing.

[Drawing 6] It is drawing showing the configuration of the encryption equipment in a WEP algorithm.

[Drawing 7] It is drawing showing the configuration of the decode equipment in a WEP algorithm.

[Drawing 8] It is drawing showing an example of a database.

[Description of Notations]

102 Wireless Transceiver Section (Information Signal Receiving Means)

103 Storage Section (Identification Information Storage Means)

105 Time Check -- Section

106 Control Section (Identification Information Setting Means, Authentication Demand Means)

107 Display (Identification Information Display Means)

SS-ID (identification information)

WEP key (cryptographic key)

STA Wireless station terminal (radio terminal unit)

AP Wireless access point

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-180010
(P2004-180010A)
(43)公開日　平成16年6月24日(2004.6.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	310	5J104
H04L 9/32	H04B 7/26	109R	5K033
H04Q 7/38	H04L 9/00	675A	5K067
	H04L 9/00	673A	

審査請求 未請求　請求項の数 1　OL　（全 15 頁）

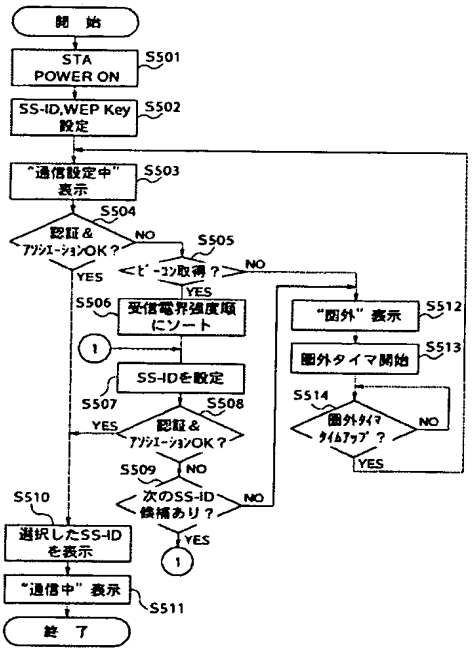
(21)出願番号　特願2002-344286(P2002-344286)
(22)出願日　平成14年11月27日(2002.11.27)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100081880
弁理士　渡部　敏彦
(72)発明者　廣瀬　崇俊
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Fターム(参考)　5J104 AA07 KA02 KA04 KA06 KA14 NA03 NA05 PA01
5K033 AA08 AA09 CB01 DA17 DB20 EA06 EA07 EC01
5K067 AA30 AA32 BB04 BB21 DD11 DD51 EE02 EE10 EE16 FF02 HH36

(54)【発明の名称】無線通信端末装置

(57)【要約】
【課題】通信を希望する無線アクセスポイントの識別情報が変更になっても、ネットワークに容易に参加することができるようにする。
【解決手段】無線ステーション端末ＳＴＡ１は、ＳＳ－ＩＤ”１１１１１”で認証要求メッセージを送出すると、”１１１１１”を保有している無線アクセスポイントＡＰ１は、ＳＴＡ１との間で認証処理を行う。ところが、それぞれに設定されているＷＥＰ鍵が異なっているので、認証拒否メッセージが返信される。次に、ＳＴＡ１は、複数のＡＰから送出されるビーコン信号を受信し、それに含まれるＳＳ－ＩＤと受信電界強度をデータベース８０１に保管し、認証処理失敗したものを除く、受信電界強度が最も大きいＳＳ－ＩＤを、新たなＳＳ－ＩＤとして選択し、新たに設定されたＳＳ－ＩＤにて認証要求を行う。



1

【特許請求の範囲】
【請求項１】
複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置であって、
認証処理用の識別情報を設定する識別情報設定手段と、
前記複数の無線アクセスポイントのうち、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、
前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信手段とを有し、
認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をすることを特徴とする無線通信端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術の分野】
本発明は、無線アクセスポイントとデータ通信を行う際の技術に関する。
【０００２】
【従来の技術】
従来、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）鍵等の同一の暗号鍵を用いて無線アクセスポイントと秘匿通信を行う無線通信端末装置が知られている。
【０００３】
例えば、下記特許文献１では、無線アクセスポイントが無線ステーション端末からの「Ｓｈａｒｅｄ　Ｋｅｙ認証」を行なった後、ネットワーク管理者に対し認証の最終的な許可を得ることで、認証処理のセキュリティレベルを向上させる技術が示されている。
【０００４】
すなわち、無線ＬＡＮシステムにおいて、図２に示すように、３つの無線アクセスポイントＡＰ１、ＡＰ２及びＡＰ３がそれぞれ稼動しており、無線通信端末装置である無線ステーション端末ＳＴＡ１がこれから通信をしようとしている場合を想定する。無線アクセスポイントＡＰ１、ＡＰ２及びＡＰ３は、システム識別情報として互いに異なるＳＳ－ＩＤ（Ｓｅｖｉｃｅ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）を保有している。各ＳＳ－ＩＤは、無線アクセスポイントＡＰ１では”１１１１１”、無線アクセスポイントＡＰ２では”２２２２２”、無線アクセスポイントＡＰ３では”３３３３３”であるとする。無線アクセスポイントＡＰ１～ＡＰ３のそれぞれの無線エリア（無線信号が届く範囲）は、２０６、２０７、２０８で示されている。無線ステーション端末ＳＴＡ１は、現在、すべての無線エリア２０６、２０７、２０８の範囲内に存在しているとする。

2

【０００５】
今、無線ステーション端末ＳＴＡ１に設定されているＳＳ－ＩＤが”１１１１１”であるとすると、無線ステーション端末ＳＴＡ１は、ＳＳ－ＩＤが共通する無線アクセスポイントＡＰ１と通信でき、”２２２２２”であるとすると無線アクセスポイントＡＰ２、さらに”３３３３３”であるとすると無線アクセスポイントＡＰ３と通信できる。また、それ以外のＳＳ－ＩＤを用いた場合には、通信相手が見つからないことになる。そのようなことは、認証シーケンスを用いることで分かる。
【０００６】
無線ＬＡＮ規格ＩＥＥＥ８０２．１１で定められた認証シーケンスは、２通り存在しており、それぞれ「Ｏｐｅｎ　Ｓｙｓｔｅｍ認証」と「Ｓｈａｒｅｄ　Ｋｅｙ認証」と呼ばれる。それぞれの大きな違いは、認証時にＷＥＰ（ＷｉｒｅｄＥｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）を用いた秘匿通信を用いるか否かである。「Ｏｐｅｎ　Ｓｙｓｔｅｍ認証」はＷＥＰを用いなくても認証シーケンスができ、「Ｓｈａｒｅｄ　Ｋｅｙ認証」はＷＥＰを用いる。
【０００７】
ここで、ＩＥＥＥ８０２．１１のＷＥＰアルゴリズムについて図６、図７を用いて説明する。
【０００８】
図６は、ＷＥＰアルゴリズムにおける暗号化装置の構成を示す図である。図７は、ＷＥＰアルゴリズムにおける復号装置の構成を示す図である。これら暗号化装置及び復号装置は、無線ステーション端末ＳＴＡ及び無線アクセスポイントＡＰに設けられる。
【０００９】
図６に示すように、暗号化装置は、入力された二つのビット列を結合し、一つのビット列にする結合器６０１、６０４を備える。擬似乱数発生器６０２は、結合器６０１の結果を種とし、擬似乱数発生アルゴリズムを用いて、より長いビット系列（鍵系列）を発生する。ＣＲＣ装置６０３は、ＣＲＣ（巡回冗長検査）アルゴリズムを用いて、ビット列に誤りが在るか否かをチェックするビット列（ＩＣＶ）を生成する。ＸＯＲ装置６０５は、入力された二つのビット系列の排他的論理和を求める。擬似乱数発生アルゴリズムとしては、ＲＳＡセキュリティ社のＲＣ４擬似乱数発生アルゴリズムが用いられる。
【００１０】
図６に示す暗号化装置には、任意のビット列である初期化系列、暗号鍵、及び暗号化されるデータが入力される。初期化系列及び暗号鍵は、結合器６０１に入力され、初期化系列及び暗号鍵を結合したビット系列である種が出力される。この種は擬似乱数発生器６０２に入力され、データの長さとＩＣＶの長さを加えた長さのビット系列である鍵系列が生成される。また、データは、ＣＲＣ装置６０３に入力されてＩＣＶが生成される。デー

タ及び生成されたＩＣＶは結合器６０４に入力され、結合される。結合器６０４から出力されるＩＣＶ及びデータの結合、並びに擬似乱数発生器６０２から出力される鍵系列は、ＸＯＲ装置６０５に入力され、ビット毎の排他的論理和がとられる。ＸＯＲ装置６０５で排他的論理和をとった結果が暗号化データとなる。そして、初期化系列と暗号化データとが一組とされ出力される。

【００１１】

また、復号装置は、図７に示すように、入力された二つのビット列を結合し、一つのビット列にする結合器７０１を備える。擬似乱数発生器７０２は、結合器７０１の結果を種とし、擬似乱数発生アルゴリズムを用いて、より長いビット系列（鍵系列）を発生する。ＸＯＲ装置７０３は、入力された二つのビット系列の排他的論理和を求める。分離器７０４は、入力されたビット列を所定の方法で、データとＩＣＶの二つのビット列に分離する。ＣＲＣ装置７０５は、ＣＲＣアルゴリズムを用いて、ＩＣＶを生成する。判定器７０６は、分離器７０４により生成されたＩＣＶとＣＲＣ装置７０５で生成されたＩＣＶを比較することにより、データが正しいか否かを判定する。擬似乱数発生アルゴリズムとしては、ＲＳＡセキュリティ社のＲＣ４擬似乱数発生アルゴリズム等が用いられる。

【００１２】

図７に示す復号装置には、暗号化データと初期化系列との組、及び暗号鍵が入力される。初期化系列及び暗号鍵は、結合器７０１に入力され、初期化系列及び暗号鍵を結合したビット系列である種が出力される。この種は擬似乱数発生器７０２に入力され、データの長さとＩＣＶの長さを加えた長さのビット系列である鍵系列が生成される。この鍵系列と上記暗号化データは、ＸＯＲ装置７０３に入力されビット毎の排他的論理和が計算される。ＸＯＲ装置７０３の計算結果は分離器７０４に入力され、所定の方法で分割されて、データとＩＣＶが生成される。このデータは出力されるとともに、ＣＲＣ装置７０５に入力されてＩＣＶが計算される。ＣＲＣ装置７０５で計算されたＩＣＶと分離器７０４により生成されたＩＣＶは、判定装置７０６に入力される。判定装置７０６では、それら二つのＩＣＶが等しければ、判定フラグとして正常復号を示すフラグを、等しくなければ、復号失敗を示すフラグを出力する。

【００１３】

このＷＥＰを認証処理に用いた「Ｓｈａｒｅｄ　Ｋｅｙ認証」のシーケンス、及び認証シーケンスに続いて行なわれるアソシエーションシーケンスについて、図３を用いて説明する。

【００１４】

まず、無線ステーション端末ＳＴＡは、認証要求メッセージ３０１を無線アクセスポイントＡＰに対して送信する。そのメッセージ３０１の中には、認証アルゴリズムとして“Ｓｈａｒｅｄ　Ｋｅｙ認証”を使うことが記される。

【００１５】

それを受けた無線アクセスポイントＡＰは、認証応答メッセージ３０２を無線ステーション端末ＳＴＡに対して送信する。そのメッセージ３０２の中には、この認証手続きの度に、任意に決めることができるＩＶ（Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒ）と、ＷＥＰ鍵の値をパラメータとし、ＷＥＰ　ＰＲＮＧ（Ｐｓｅｕｄｏ　ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）のアルゴリズムに従い数値演算を行い、１２８オクテットの一意に決まるＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を算出したものとが含まれる。

【００１６】

Ｃｈａｌｌｅｎｇｅ　Ｔｅｘｔを含んだメッセージ３０２を受信した無線ステーション端末ＳＴＡは、Ｃｈａｌｌｅｎｇｅ　Ｔｅｘｔデータに対して、ＷＥＰ暗号化アルゴリズムに従って暗号化を行い、その暗号化データを認証要求メッセージ３０３として、無線アクセスポイントＡＰに送信する。

【００１７】

そのメッセージ３０３を受信した無線アクセスポイントＡＰは、通知されたＩＶと、予め知っているＷＥＰ鍵データとを基に暗号化データを復号化する。そして、復号化した際の出力ＩＣＶと、通知されたＩＣＶが同一であれば、認証許可とし、無線ステーション端末ＳＴＡに認証応答メッセージ３０４として送信する。

【００１８】

その結果、認証許可であれば、無線ステーション端末ＳＴＡは、次のアソシエーションの手順に入ることができ、認証拒否の場合は、認証失敗ということで、アソシエーション手続きを行うことができない。

【００１９】

次に、認証シーケンスに続いて行なわれるアソシエーションシーケンスについて説明する。

【００２０】

図３に示すように、無線ステーション端末ＳＴＡは、アソシエーション要求メッセージ３０５を無線アクセスポイントＡＰに送信する。

【００２１】

アソシエーション要求メッセージ３０５中のＳＳ－ＩＤを受信した無線アクセスポイントＡＰは、上記ＳＳ－ＩＤにより無線ステーション端末ＳＴＡを識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定する。そして、許可する場合はアソシエーション許可のアソシエーション応答メッセージ３０６を無線ステーション端末ＳＴＡに送信する。

【００２２】

このように処理されることで、無線アクセスポイントＡ

5

Ｐと無線ステーション端末ＳＴＡ間の無線リンクが張れ（データリンク確立３０７）、通信が可能になるのである。つまり、この認証・アソシエーション方法によれば、無線アクセスポイントＡＰと無線ステーション端末ＳＴＡが、予めＳＳ－ＩＤと、ＷＥＰ鍵を持ち合うことで、無線アクセスポイントＡＰが特定の無線ステーション端末ＳＴＡに対して認証・アソシエーションを許可する仕組みが実現される。

【００２３】

【特許文献１】

特開２００１－３４５８１９号公報

【００２４】

【発明が解決しようとする課題】

しかしながら、上記特許文献１等で示される従来の認証・アソシエーション手法では、それぞれ同一のＳＳ－ＩＤ及びＷＥＰ鍵を、無線アクセスポイントＡＰと無線ステーション端末ＳＴＡとが持ち合うことにより無線通信が行えるが、実際には、無線アクセスポイントＡＰ設置の際にＳＳ－ＩＤが他のＳＳ－ＩＤと重なっていた等の理由により、無線アクセスポイントＡＰにおけるＳＳ－ＩＤの設定が変更されることがある。そして、そのような場合であっても無線ステーション端末ＳＴＡ側ではその変更を知らないのが通常であるため、無線通信を行うことが不可能となり、ネットワークへの参加が容易でないという問題があった。

【００２５】

本発明は上記従来技術の問題を解決するためになされたものであり、その目的は、通信を希望する無線アクセスポイントの識別情報が変更になっても、ネットワークに容易に参加することができるようにすることにある。

【００２６】

【課題を解決するための手段】

上記目的を達成するために本発明の請求項１の無線通信端末装置は、複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置であって、認証処理用の識別情報を設定する識別情報設定手段と、前記複数の無線アクセスポイントのうち、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信手段とを有し、認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をすることを特徴とする。

【００２７】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。

【００２８】

6

図１は、本発明の一実施の形態に係る無線通信端末装置の構成を示すブロック図である。無線通信端末装置である無線ステーション端末ＳＴＡは、無線送受信部１０２（報知信号受信手段）、記憶部１０３（識別情報記憶手段）、ネットワークインタフェース処理部１０４、計時部１０５、制御部１０６（識別情報設定手段、認証要求手段）及び表示部１０７（識別情報表示手段）を備える。

【００２９】

なお、無線ステーション端末ＳＴＡ及び無線アクセスポイントＡＰは、図６、図７に示す暗号化装置及び復号装置を有している。また、各無線ステーション端末ＳＴＡ同士、各無線アクセスポイントＡＰ同士は同様に構成される。

【００３０】

図２は、無線ステーション端末ＳＴＡ及び無線アクセスポイントＡＰで構築される無線ＬＡＮシステムの構成図である。本実施の形態では、無線会議システムとして無線ＬＡＮを用いる例について述べる。

【００３１】

図示はしないが、無線ステーションＳＴＡ２は、パーソナルコンピュータ（ＰＣ）と接続され、さらにプロジェクタとも接続されており、ＰＣ画面をスクリーン等に映写できるものとする。

【００３２】

また、無線会議の参加者は、それぞれＰＣに接続された無線ステーション端末ＳＴＡを持っているが、以降の説明では、参加者は無線ステーション端末ＳＴＡ１のユーザ１名のみであるとする。また、無線会議システムの無線アクセスポイントは、無線アクセスポイントＡＰ３であるとし、その他の無線アクセスポイントとして、無線アクセスポイントＡＰ１、無線アクセスポイントＡＰ２が稼動している。

【００３３】

本実施の形態では、無線ステーション端末ＳＴＡ１のユーザが、無線アクセスポイントＡＰ３を経由して無線ステーション端末ＳＴＡ２に接続されたプロジェクタを用いてプレゼンテーションをする場合における、無線アクセスポイントＡＰ３－無線ステーション端末ＳＴＡ１間の認証・アソシエーション手順について説明する。なお、本無線会議では、当初、無線アクセスポイントＡＰ３に設定されているＳＳ－ＩＤとして”１１１１１”を使うこととする。

【００３４】

また、本実施の形態では、無線ＬＡＮ規格ＩＥＥＥ８０２．１１で定められた認証シーケンスのひとつである、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）を用いた「Ｓｈａｒｅｄ　Ｋｅｙ認証」により認証を行うものとする。図６、図７に示した暗号化装置及び復号装置は、各無線ステーション端末ＳＴＡ及び各

無線アクセスポイントＡＰに設けられるものとする。なお、ＷＥＰアルゴリズムについては、図６、図７で上述した通りである。

【００３５】

まず、会議に先立って、無線アクセスポイントＡＰ３と無線ステーション端末ＳＴＡ１は、それぞれ必要項目について設定する。必要設定項目は、ＳＳ－ＩＤやＷＥＰ鍵（暗号鍵）等である。ＷＥＰ鍵については、無線アクセスポイントＡＰ３と無線ステーション端末ＳＴＡ１とで同一のものが設定される。設定には様々な方法が可能であり、無線アクセスポイントＡＰ３と無線ステーション端末ＳＴＡ１が別々に行うこともできる。また、会議場所でなくても設定することは可能である。

【００３６】

ここで、無線アクセスポイントＡＰ３には、会議場所に行くまではＳＳ－ＩＤとして”１１１１１”が設定されていたが、会議場所の付近でＳＳ－ＩＤ”１１１１１”というものが無線アクセスポイントＡＰ１によって使用されていたので、急遽、無線アクセスポイントＡＰ３のＳＳ－ＩＤを”３３３３３”に変更した場合を想定する。その結果、それぞれの無線アクセスポイントＡＰのＳＳ－ＩＤは、無線アクセスポイントＡＰ１では”１１１１１”、無線アクセスポイントＡＰ２では”２２２２２”、そして無線アクセスポイントＡＰ３では”３３３３３”となった。無線アクセスポイントＡＰ３でのＳＳ－ＩＤの変更は、当然、無線ステーション端末ＳＴＡ１には知らされていない。

【００３７】

かかる状況において、無線ステーション端末ＳＴＡ１が無線会議に参加する場合の処理を図４、図５を用いて説明する。

【００３８】

図４は、認証・アソシエーション処理のシーケンスを示し、図５は、認証・アソシエーション処理のフローチャートを示す。図５の処理は、制御部１０６により実行される。以降、両者を参照して説明する。

【００３９】

会議場所に無線アクセスポイントＡＰ３が設置され、無線アクセスポイントＡＰ３が稼動している状態で、まず、会議場所に無線ステーション端末ＳＴＡ１が来て、その電源をＯＮする（４０１、ステップＳ５０１）。そして、無線ステーション端末ＳＴＡ１に、ＳＳ－ＩＤ、ＷＥＰ鍵等が予め設定されていない場合はそれらの設定を行う（ステップＳ５０２）。

【００４０】

次に、無線ステーション端末ＳＴＡ１では、無線アクセスポイントＡＰとの無線リンクを張るための準備をしている状態であることを無線ステーション端末ＳＴＡ１のユーザに通知するために、表示部１０７に「通信設定中」の表示をさせる（ステップＳ５０３）。また、記憶

部１０３に記憶されている後述するデータベース８０１（図８参照）の内容の全消去を行う。ここで、無線ステーション端末ＳＴＡ１のＳＳ－ＩＤは、当初の予定の”１１１１１”に設定されている。

【００４１】

図８は、データベース８０１の一例を示す図である。データベース８０１には、後述するビーコン信号（報知信号）の受信等により得られた無線アクセスポイントＡＰのＳＳ－ＩＤに、その受信電界強度が対応付けられて記憶されると共に、そのＳＳ－ＩＤを用いて認証処理が失敗した場合は、認証処理失敗を示す情報が対応付けられて記憶される。

【００４２】

図４、図５に戻り、次に、無線ステーション端末ＳＴＡ１は、無線リンクを張るために、認証要求を行う（４０２）。これらの処理は、図３で上述した手順でなされる。すなわち、Ｓｈａｒｅｄ　Ｋｅｙ認証を選択し、ＳＳ－ＩＤ”１１１１１”で認証要求メッセージを送出する（４０２）。そして、認証及びアソシエーションが許可されたか否かを判別する（ステップＳ５０４）。

【００４３】

これに対し、ＳＳ－ＩＤ”１１１１１”を保有している無線アクセスポイントＡＰ１は、送出された認証要求メッセージ（４０２）を受信し、無線ステーション端末ＳＴＡ１との間で認証処理を行う。

【００４４】

ところが、無線ステーション端末ＳＴＡ１と無線アクセスポイントＡＰ１とでは、それぞれに設定されているＷＥＰ鍵が異なっているので、無線アクセスポイントＡＰ１は無線ステーション端末ＳＴＡ１に対して認証拒否メッセージを送信する（４０３）。

【００４５】

従って、この場合は、前記ステップＳ５０４の判別の結果、「ＮＯ」となる。そして、無線ステーション端末ＳＴＡ１の記憶部１０３にあるデータベース８０１に、認証失敗の無線アクセスポイントＡＰ１のＳＳ－ＩＤ”１１１１１”を認証処理失敗のチェックとともに保管する。そして、計時部１０５により計時を開始する（４０４）。

【００４６】

次に、無線ステーション端末ＳＴＡ１は、複数の無線アクセスポイントＡＰから送出されるビーコン信号を受信するスキャニング（Ｓｃａｎｎｉｎｇ）動作（４０７）を、タイマが終了（４０９）するまで行う。ここでは、無線アクセスポイントＡＰ１～ＡＰ３のすべての無線アクセスポイントＡＰから発信されるビーコン信号が受信される。

【００４７】

このスキャニング動作（４０７）では、受信ビーコン信号に含まれる無線アクセスポイントＡＰのＳＳ－ＩＤと

受信電界強度が、無線ステーション端末ＳＴＡ１の記憶部１０３にあるデータベース８０１に保管される（４０５、４０６、４０８）。データベース８０１に、データがある場合は、そのデータとＯＲを取る。

【００４８】

ステップＳ５０５では、ビーコン信号が受信されたか否かを判別し、ビーコン信号を受信できない場合は、表示部１０７に「圏外」表示させて（ステップＳ５１２）、無線アクセスポイントＡＰが存在しないことを無線ステーション端末ＳＴＡ１のユーザに通知する。

【００４９】

一方、ビーコン信号が受信できた場合は、ＳＳ－ＩＤをその受信電界強度順に並び替え（ステップＳ５０８）、受信電界強度が最も大きいＳＳ－ＩＤを、無線ステーション端末ＳＴＡ１に設定するＳＳ－ＩＤとして選択し、設定する（ステップＳ５０７）。ただし、データベース８０１の認証処理失敗の欄にチェックが付いているＳＳ－ＩＤが存在する場合は、それを用いた認証処理は行わない。図８の例では、ＳＳ－ＩＤ”１１１１１”を用いた認証処理は行わない。すなわち、認証処理失敗に係るＳＳ－ＩＤを除いたもののうち受信電界強度が最も大きいＳＳ－ＩＤが選択される。その結果、図８の例では、ＳＳ－ＩＤ”２２２２２”が選択・設定される。

【００５０】

次に、無線ステーション端末ＳＴＡ１は、無線リンクを張るために、新たに設定されたＳＳ－ＩＤにて認証要求を行う（４１０）。すなわち、Ｓｈａｒｅｄ　Ｋｅｙ認証を選択し、ＳＳ－ＩＤ”２２２２２”で認証要求メッセージを送出する（４１０）。そして、認証及びアソシエーションが許可されたか否かを判別する（ステップＳ５０８）。

【００５１】

これに対し、ＳＳ－ＩＤ”２２２２２”を保有している無線アクセスポイントＡＰ２は、送出された認証要求メッセージ（４１０）を受信し、無線ステーション端末ＳＴＡ１との間で認証処理を行う。

【００５２】

ところが、無線ステーション端末ＳＴＡ１と無線アクセスポイントＡＰ２とでは、それぞれに設定されているＷＥＰ鍵が異なっているので、無線アクセスポイントＡＰ２は、無線アクセスポイントＡＰ１の場合と同様に、無線ステーション端末ＳＴＡ１に対して認証拒否メッセージを送信する（４１１）。

【００５３】

従って、この場合は、前記ステップＳ５０８の判別の結果、「ＮＯ」となる。そして、無線ステーション端末ＳＴＡ１の記憶部１０３にあるデータベース８０１に、認証失敗の無線アクセスポイントＡＰ２のＳＳ－ＩＤ”２２２２２”を認証処理失敗のチェックとともに保管する。データベース８０１にデータがある場合は、そのデータとＯＲを取る。

【００５４】

次に、データベース８０１を参照し、次のＳＳ－ＩＤ候補が存在するか否かを判別する（ステップＳ５０９）。すなわち、データベース８０１に認証処理失敗のチェックがついていない他のＳＳ－ＩＤがあるかどうかの確認を行う。

【００５５】

その判別の結果、次のＳＳ－ＩＤの候補が存在しない場合は、表示部１０７に「圏外」表示をさせることで（ステップＳ５１２）、通信できる無線アクセスポイントＡＰが存在しないことを無線ステーション端末ＳＴＡ１ユーザに通知する。

【００５６】

次に、ステップＳ５１３では、計時部１０５により圏外タイマ計時を開始し、圏外タイマがタイムアップしたか否かを判別する（ステップＳ５１４）。

【００５７】

圏外タイマがタイムアップするまでその判別を繰り返し、圏外タイマがタイムアップした場合は、前記ステップＳ５０３に戻って、表示部１０７に「通信設定中」の表示をさせることで、再度の認証処理に移行する。これにより、圏外タイマにより無線ステーション端末ＳＴＡ１が圏外になった場合でも、すぐには再認証処理が行われず、一定時間の経過を待つので、バッテリや電波の送出を抑えることができる。

【００５８】

前記ステップＳ５０９の判別の結果、次のＳＳ－ＩＤの候補が存在する場合は、前記ステップＳ５０７に戻る。この場合は、ＳＳ－ＩＤ”３３３３３”が選択、設定される。そして、同様に、無線ステーション端末ＳＴＡ１は、認証及びアソシエーション処理に移行する（４１２）。これらの処理は、図３で上述した手順でなされる。まず、無線リンクを張るために、認証要求を行う。すなわち、Ｓｈａｒｅｄ　Ｋｅｙ認証を選択し、ＳＳ－ＩＤ”３３３３３”で認証要求メッセージを送出し、認証及びアソシエーションが許可されたか否かを判別する（ステップＳ５０８）。

【００５９】

これに対し、ＳＳ－ＩＤ”３３３３３”を保有している無線アクセスポイントＡＰ３は、送出された認証要求メッセージを受信し、無線ステーション端末ＳＴＡ１との間で認証処理を行う。

【００６０】

ここで、無線ステーション端末ＳＴＡ１と無線アクセスポイントＡＰ３とでは、それぞれに設定されているＷＥＰ鍵が同一であるので、無線アクセスポイントＡＰ３は無線ステーション端末ＳＴＡ１に対して認証許可メッセージを送信する。さらに、無線ステーション端末ＳＴＡ１と無線アクセスポイントＡＰ３とは、アソシエーショ

ン処理を行う。これにより、無線データリンクが確立する（４１３）。

【００６１】

すると、前記ステップＳ５０８で、「ＹＥＳ」となり、無線ステーション端末ＳＴＡ１では、表示部１０７に、「選択したＳＳ－ＩＤ」を表示させる（ステップＳ５１０）。その後、表示部１０７に、「通信中」を表示させて（ステップＳ５１１）、本処理を終了する。

【００６２】

なお、前記ステップＳ５０４の判別の結果、「ＹＥＳ」と判別された場合は、前記ステップＳ５１０、Ｓ５１１を実行して本処理を終了する。

【００６３】

本実施の形態によれば、無線ステーション端末ＳＴＡが無線アクセスポイントＡＰから送出されるビーコン信号中のＳＳ－ＩＤを受信することにより、無線アクセスポイントＡＰに設定されているＳＳ－ＩＤがわかり、ＩＥＥＥ８０２．１１のＳｈａｒｅｄ　Ｋｅｙ認証を行うことによりＷＥＰ鍵の正誤がわかるので、通信したい無線アクセスポイントＡＰのＳＳ－ＩＤが変更されたとしても、その無線アクセスポイントＡＰとの認証・アソシエーションを容易に確保することができる。従って、必ずしもＳＳ－ＩＤを設定する必要性がなくなり、ネットワークに容易に参加できるようになる。

【００６４】

なお、本実施の形態では、無線会議システムでの場合について例示したが、無線会議システムでない場合における無線通信についても、同様の手法を適用することができる。また、タイマや表示部が存在しない無線ステーションでも有効である。

【００６５】

また、受信電界強度が最も大きいＳＳ－ＩＤから、新たに設定するＳＳ－ＩＤとして選択する以外にも、受信したＳＳ－ＩＤをランダムに新たに設定するＳＳ－ＩＤとして選択する等の方法が考えられる。

【００６６】

なお、本実施の形態では、無線ステーション端末ＳＴＡ１が無線アクセスポイントＡＰ３との間での認証及びアソシエーション処理を例示したが、他の無線ステーション端末ＳＴＡ及び無線アクセスポイントＡＰ間についても同様に処理される。

【００６７】

また、本発明の目的は、実施の形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）が記憶媒体に格納されたプログラムコードを読み出して実行することによっても達成される。

【００６８】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施の形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００６９】

又、プログラムコードを供給するための記憶媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００７０】

また、コンピュータが読み出したプログラムコードを実行することにより、上記実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７１】

更に、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７２】

本発明の様々な例と実施例が示され説明されたが、当業者であれば、本発明の趣旨と範囲は本明細書の特定の説明と図に限定されるのではなく、本願特許請求の範囲にすべて述べられた様々の修正と変更に及ぶことが理解されるであろう。

【００７３】

本発明の実施態様の例を以下に列挙する。

【００７４】

〔実施態様１〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置であって、認証処理用の識別情報を設定する識別情報設定手段と、前記複数の無線アクセスポイントのうち、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信手段とを有し、前記識別情報設定手段は、前記報知信号受信手段により受信された報知信号中の識別情報を、前記認証処理用の識別情報として設定することを特徴とする無線通信端末装置。

【００７５】
〔実施態様２〕　前記報知信号受信手段は、前記認証要求手段による認証要求に対し、前記無線アクセスポイントから認証が得られなかった場合に、前記報知信号を受信することを特徴とする実施態様１記載の無線通信端末装置。
【００７６】
〔実施態様３〕　前記識別情報設定手段は、複数の無線アクセスポイントから報知信号が受信された場合は、前記報知信号が受信される際の受信電界強度に基づいて、前記認証処理用の識別情報として設定に用いる識別情報を選択することを特徴とする実施態様１または２記載の無線通信端末装置。
【００７７】
〔実施態様４〕　前記報知信号受信手段により受信された報知信号中の識別情報を記憶する識別情報記憶手段を有し、前記識別情報設定手段は、前記認証要求手段による認証要求に対し、前記無線アクセスポイントから認証が得られなかった場合は、前記識別情報記憶手段により記憶された識別情報のうち、前回以前に認証処理用の識別情報として設定されていた識別情報とは異なる識別情報を、新たな認証処理用の識別情報として再設定することを特徴とする実施態様１～３のいずれかに記載の無線通信端末装置。
【００７８】
〔実施態様５〕　前記識別情報設定手段が、前記識別情報記憶手段により記憶された識別情報のすべてについて、前記新たな認証処理用の識別情報としての再設定を行い、且つ前記認証要求手段が認証要求を行った結果、いずれの無線アクセスポイントからも認証が得られなかった場合は、前記報知信号受信手段は、一定時間経過後に、前記報知信号の受信を再度やり直すことを特徴とする実施態様４記載の無線通信端末装置。
【００７９】
〔実施態様６〕　前記認証要求手段による認証要求に対し、前記無線アクセスポイントから認証が得られた場合は、その際に前記識別情報設定手段により設定されている識別情報を表示する識別情報表示手段を有することを特徴とする実施態様１～５のいずれかに記載の無線通信端末装置。
【００８０】
〔実施態様７〕　前記無線アクセスポイントによる認証は、無線規格ＩＥＥＥ８０２．１１で定められたＳｈａｒｅｄ　Ｋｅｙ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎに従ってなされることを特徴とする実施態様１～６のいずれかに記載の無線通信端末装置。
【００８１】
〔実施態様８〕　前記秘匿通信は、無線規格ＩＥＥＥ８０２．１１で定められたＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）によりなされることを特徴とする実施態様１～７のいずれかに記載の無線通信端末装置。
【００８２】
〔実施態様９〕　複数の無線アクセスポイントと、前記複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置とが接続された無線通信システムであって、前記複数の無線アクセスポイントは、前記無線通信端末装置からの認証要求に応じて、前記暗号鍵を用いて認証を行う認証手段と、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を発信する報知信号発信手段とを有し、前記無線通信端末装置は、認証処理用の識別情報を設定する識別情報設定手段と、前記複数の無線アクセスポイントのうち、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、前記複数の無線アクセスポイントから発信される前記報知信号を受信する報知信号受信手段とを有し、前記識別情報設定手段は、前記報知信号受信手段により受信された報知信号中の識別情報を、前記認証処理用の識別情報として設定することを特徴とする無線通信システム。
【００８３】
〔実施態様１０〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信方法であって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信ステップとを有し、前記識別情報設定ステップは、前記報知信号受信ステップにより受信された報知信号中の識別情報を、前記認証処理用の識別情報として設定することを特徴とする通信方法。
【００８４】
〔実施態様１１〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信プログラムであって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受

信ステップとをコンピュータに実行させるプログラムであり、前記識別情報設定ステップは、前記報知信号受信ステップにより受信された報知信号中の識別情報を、前記認証処理用の識別情報として設定することを特徴とする通信プログラム。

【００８５】

〔実施態様１２〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信プログラムを記憶したコンピュータ読み取り可能な記憶媒体であって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信ステップとをコンピュータに実行させるプログラムを記憶し、前記識別情報設定ステップは、前記報知信号受信ステップにより受信された報知信号中の識別情報を、前記認証処理用の識別情報として設定することを特徴とする記憶媒体。

【００８６】

〔実施形態１３〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置であって、認証処理用の識別情報を設定する識別情報設定手段と、前記複数の無線アクセスポイントのうち、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信手段とを有し、認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をすることを特徴とする無線通信端末装置。

【００８７】

〔実施形態１４〕　無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記無線アクセスポイントと秘匿通信を行う無線通信端末装置であって、認証処理用の識別情報を設定する識別情報設定手段と、前記識別情報設定手段により設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求手段と、他の無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信手段とを有し、前記無線アクセスポイントとの認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をすることを特徴とする無線通信端末装置。

【００８８】

〔実施態様１５〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信方法であって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信ステップと、認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をする認証処理ステップとを有することを特徴とする無線通信端末装置における通信方法。

【００８９】

〔実施態様１６〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信プログラムであって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信ステップと、認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をする認証処理ステップとをコンピュータに実行させることを特徴とする通信プログラム。

【００９０】

〔実施態様１７〕　複数の無線アクセスポイントのうち所望の無線アクセスポイントが保有する暗号鍵と同一の暗号鍵を用いて、前記所望の無線アクセスポイントと秘匿通信を行う無線通信端末装置における通信プログラムを記憶したコンピュータ読み取り可能な記憶媒体であって、認証処理用の識別情報を設定する識別情報設定ステップと、前記複数の無線アクセスポイントのうち、前記識別情報設定ステップにより設定された識別情報に対応する無線アクセスポイントに対して認証要求する認証要求ステップと、前記複数の無線アクセスポイントから発信される、各無線アクセスポイントに設定されている識別情報を含んだ報知信号を受信する報知信号受信ステップと、認証処理に失敗した場合は、前記報知信号受信手段で受信した識別情報に設定を変更して認証処理をする認証処理ステップとをコンピュータに実行させるプログラムを記憶したことを特徴とする記憶媒体。

17

【００９１】

【発明の効果】

以上説明したように、本発明によれば、通信を希望する無線アクセスポイントの識別情報が変更になっても、報知信号から取得した識別情報で認証を得ることで、ネットワークに容易に参加することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る無線通信端末装置の構成を示すブロック図である。

【図２】無線ステーション端末ＳＴＡ及び無線アクセスポイントＡＰで構築される無線ＬＡＮシステムの構成図である。

【図３】ＷＥＰを認証処理に用いた「Ｓｈａｒｅｄ　Ｋｅｙ認証」のシーケンス、及び認証シーケンスに続いて行なわれるアソシエーションシーケンスを示す図である。

【図４】認証・アソシエーション処理のシーケンスを示す図である。

18

【図５】認証・アソシエーション処理のフローチャートを示す図である。

【図６】ＷＥＰアルゴリズムにおける暗号化装置の構成を示す図である。

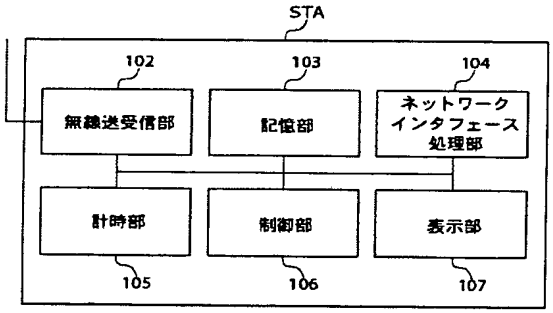
【図７】ＷＥＰアルゴリズムにおける復号装置の構成を示す図である。

【図８】データベースの一例を示す図である。

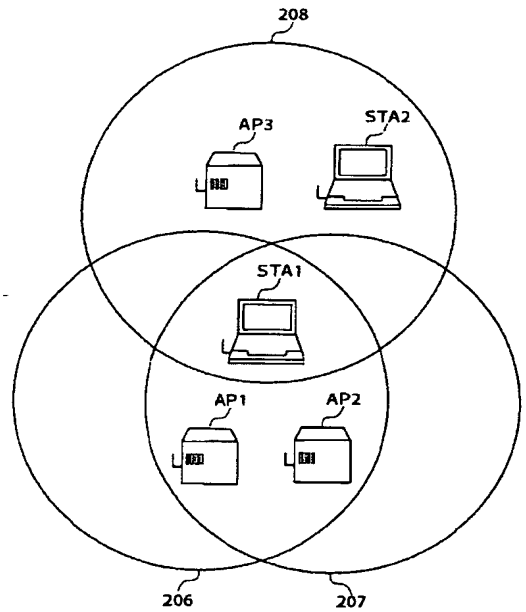
【符号の説明】

１０２　無線送受信部（報知信号受信手段）
１０３　記憶部（識別情報記憶手段）
１０５　計時部
１０６　制御部（識別情報設定手段、認証要求手段）
１０７　表示部（識別情報表示手段）
ＳＳ－ＩＤ　（識別情報）
ＷＥＰ鍵　（暗号鍵）
ＳＴＡ　無線ステーション端末（無線通信端末装置）
ＡＰ　無線アクセスポイント

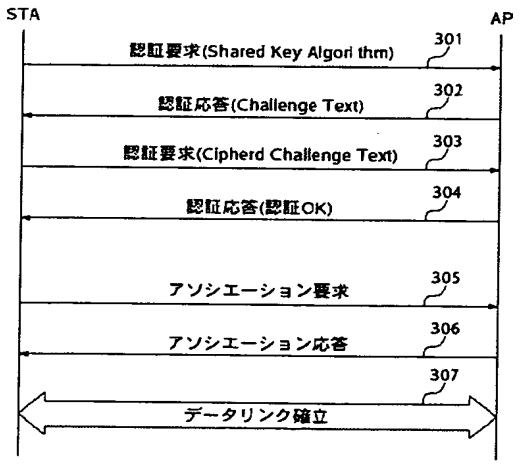
【図１】



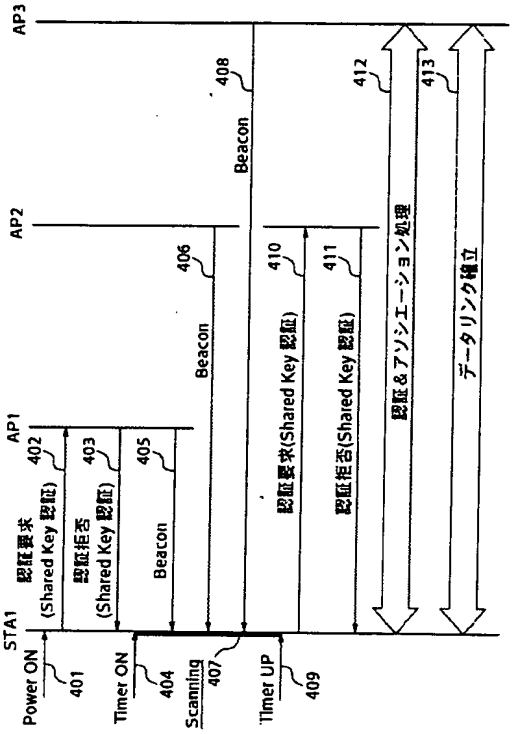
【図２】



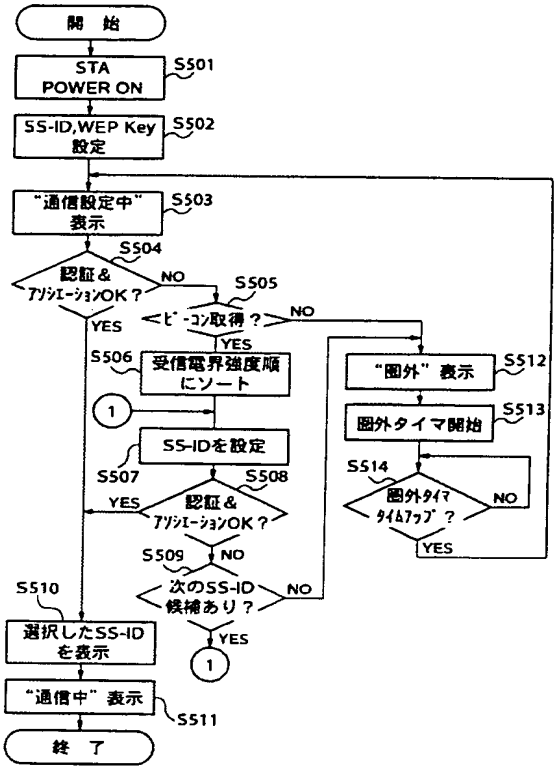
【図３】



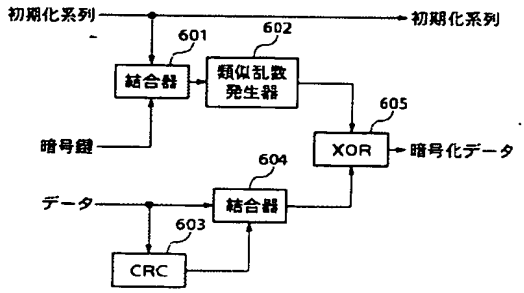
【図４】



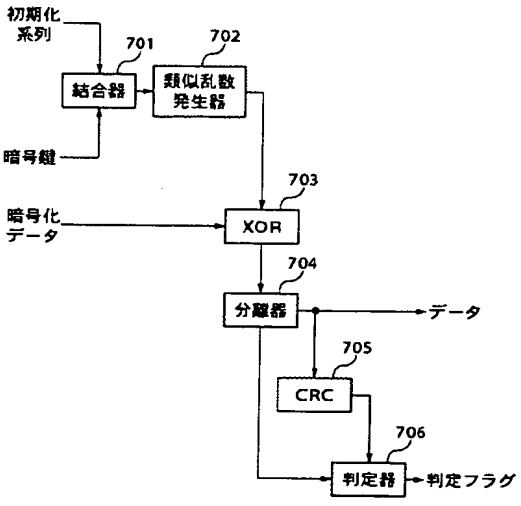
【図５】



【図６】



【図７】



【図８】

801

SS-ID	受信電界強度	認証処理失敗
11111	80	○
22222	74	－
33333	66	－
------	------	－
------	------	－